Debunking IPv6 Security Myths

Navaneethan C. Arjuman
nava@nav6.usm .my
National Advanced IPv6 Centre
April 2012

National Advanced IPv6 Centre of Excellence

Concerns

- How will IPv6 affect the organization's network?
- How secure is IPv6 compared to IPv4?
- How to implement security practices similar to IPv4?
- Are the current devices capable of blocking and filtering IPv6 traffics?

IPv6 Is Neither A Magic Bullet, Nor A Poison Pill

"If we do deploy IPv6, will it hurt us or benefit us when it comes to security?"

Its 50-50, but end of the day, you still have to deploy IPv6! (i.e. Address depletion)

"Security" should not be the reason for NOT deploying IPv6

Be skeptical to "Snake oil" claims that IPv6 improves your network's security

Myth # 1

Myth #1.

"IPv6 is more secure than IPv4, since security was considered during the design of the protocol, rather than as an afterthought."

Myth # 1

•Early specification of IPv6

- IPSec made mandatory for IPv6

- Expected IPv6+IPSec widely deployed in the short term

- Vendors wouldn't bother to add IPSec support to IPv4 implementations

• Assumptions proved to be false
- iPv4+IPsec was deployed much earlier than any significant level of deployment of IPv6

Myth # 1

• Network address translation (NAT)
-prevented the deployment of IPSec for end-to-end security.

- IPSec become ubiquitous in IPv6

• Assumptions proved to be false
- since many (if not most) of the factors that have prevented widespread deployment of IPSec for general use with IPv4 (such as the requirement for a Public Key Infrastructure) remain the same for IPv6

Myth # 2

Myth #2: "IPv6 will return the end-to-end principle to the Internet, and hence security architectures will switch from mostly network-centric, to host-centric."

Myth # 2

• IPv6-only Internet where no IPv6 NATs are deployed would return the end-to-end principle to the Internet

- network simply forwards datagrams from a source host to a destination host

- In IPv4 Internet, this principle is violated by a number of devices, with IPv4 NATs probably being the most popular and most widely deployed

Myth # 2

• One of the core design principles of the Internet is usually referred to as the "end-to-end principle"

- For many security administrators or users, the end-to-end principle is not necessarily a desired property

- Administrators may not necessarily be willing to have every host on a network be directly reachable from any arbitrary host on the Internet, an unintended consequence with IPv6 that could make a network more vulnerable to outside attackers

Myth # 2

-Typical IPv6 subnet will most likely need to be protected by a stateful firewall that only allows communications originating from the inside network

- In terms of packet filtering, the architecture of the typical IPv6 subnet will be no different from that of the typical IPv4 subnet

Myth # 3

Myth #3:
"IPv6 networks will be NAT-free."

Myth # 3

- This myth is closely related to myth #2

-Since IPv6 provides plenty of address space, NATs will not be deployed in IPv6 networks

- Coexistence with IPv4 and the transition to an IPv6-only Internet, there has been increased use of NATs

- Since most transition/coexistence technologies do not relieve hosts from the need of IPv4 addresses, the so-called Carrier-Grade NATs (CGNs) will most likely be widely deployed, thus leading to an increased use of NATs in the IPv4 Internet

Myth # 3

- On the other hand, the only transition/co-existence technology that relieves networks of the need of IPv4 addresses is NAT64

- NAT64 which allows IPv6-only nodes to communicate with IPv4-only nodes, but introduces yet another type of NAT, both in the IPv4 Internet and the IPv6 Internet.

- Network address translation – port translation (NAT-PTs) in the IPv6 Internet deserves a careful analysis as well

-IPv4 NATs were introduced as a stop-gap for IPv4 address consumption

National Advanced IPv6 Centre of Excellence

Myth # 3

- IPv4 NATs are usually perceived as providing benefits in the area of host/network masquerading, and blocking incoming connections to the internal network

- NAT device will only allow communications initiated from the internal network

-It can be argued that blocking incoming connections can be easily achieved with a normal stateful firewall (without performing address and port translation)

- Host/network masquerading does not add much in terms of security

Myth # 3

- IPv4 NATs are usually perceived as providing benefits in the area of host/network masquerading, and blocking incoming connections to the internal network

- It is also true that humans tend to resist change

- Some network administrators architect their IPv6 subnets to parallel their IPv4 subnets, i.e., deploying a IPv6 NAT-PT to act as a gateway to the Internet for the internal nodes

- So it seems in most IPv6 network architecture scenarios, NAT is likely to remain in some form.

National Advanced IPv6 Centre of Excellence

Myth # 4

Myth #4: "The vast IPv6 address space will make IPv6 address scans unfeasible."

Myth # 4

- It is assumed that the increased IPv6 address space will make IPv6 address scans unfeasible.

- this statement is made based on two assumptions that are not necessarily true in all cases

- First, it is assumed that host IPv6 addresses will be uniformly distributed over the whole address space assigned to the corresponding subnet

- Secondly, it's assumed an attacker will perform address scanning using a brute-force approach

National Advanced IPv6 Centre of Excellence

Myth # 4

- Studies of the policies used to assign IPv6 addresses indicate they are not uniformly distributed

- Rather they follow specific patterns, such as those resulting from stateless auto-configuration (SLAAC), manual configuration or use of IPv6 transition/ coexistence technologies

- It has already been found in the wild that attackers are not performing IPv6 address scans with a brute-force approach

Myth # 4

- They are trying to improve their scans by taking advantage of these known patterns of IPv6 address assignments

- The IPv6 address scans typically be more “educated”

- Attackers will employ other network reconnaissance strategies, such as identifying “alive” hosts from the IPv6 addresses leaked out by application-layer protocols (e.g., in email headers), possibly in combination with use of popular Web search engines

National Advanced IPv6 Centre of Excellence

QUESTIONS

Thank You